Amendments to the Claims

No claims are amended with this Response. The following listing of claims will replace all prior versions, and listings of claims in the application.

1. (Original) An encryption/decryption circuit comprising:

a staged pipelined logic circuit adapted to perform in series stages of encryption/decryption operations on a stage data block of a first selected width utilizing an encryption/decryption key of the first selected width and to provide an output data block of the first selected width, comprising a subsequent stage input data block input to a subsequent stage of the staged pipelined logic circuit;

a stage input data block buffer adapted to hold the stage input data block for input into a stage of the staged pipelined logic circuit, the input data block having the first selected width;

an encryption circuit adapted to encrypt the stage input data block into a encrypted stage input data block having the first selected width, the encrypted stage input data block comprising a unique combination of data bits for each unique combination of data bits in the stage input data block of the first selected width, and the encrypted stage input data block forming an input to a stage substitution circuit, the output of the stage substitution circuit forming a first subsequent stage input data block for a subsequent stage of the staged pipelined logic circuit;

a decryption circuit adapted to decrypt the stage input data block into a decrypted stage input data block having the first selected width, the decrypted stage input data block comprising a unique combination of data bits for each unique combination of data bits in the stage input data block of the first selected width that is the inverse of the encryption performed by the encryption circuit, the decrypted stage input data block forming a second subsequent stage input to the substitution circuit; and,

a first selector circuit adapted to select as the input to the substitution circuit the first or the second input.

2. (Original) The apparatus of claim 1, further comprising: a second selector circuit adapted to select as the subsequent stage input data block for the subsequent stage of the staged pipelined logic circuit the output of the substitution circuit or the stage input data block.

3. (Original) The apparatus of claim 1 further comprising: the staged pipelined logic circuit being further adapted to perform in series the stages of the encryption/decryption operations in a first plurality of stages of the staged pipelined logic circuit, each of the stages of the first plurality of stages comprising a round, and to repeat this operation for a selected number of times and for a selected number of rounds each of the selected number of times, to thereby effect a total number of rounds.

4. (Original) The apparatus of claim 2 further comprising: the staged pipelined logic circuit being further adapted to perform in series the stages of the encryption/decryption operations in a first plurality of stages of the staged pipelined logic circuit, each of the stages of the first plurality of stages comprising a round, and to repeat this operation for a selected number of times and for a selected number of rounds each of the selected number of times, to thereby effect a total number of rounds.

5. (Original) The apparatus of claim 3 further comprising: the staged pipelined logic circuit being further adapted to perform in any given one of the first plurality of times less than the first plurality of rounds depending upon the total number of rounds necessary.

6. (Original) The apparatus of claim 4 further comprising: the staged pipelined logic circuit being further adapted to perform in any given one of the first plurality of times less than the first plurality of rounds depending upon the total number of rounds necessary.

7. (Original) The apparatus of claim 1 further comprising: a round key generation circuit adapted to provide a round encryption or decryption key of the first selected width for combination

with the block data of the first selected width, based upon an initial encryption or decryption key of a second selected width.

8. (Original) The apparatus of claim 2 further comprising: a round key generation circuit adapted to provide a round encryption or decryption key of the first selected width for combination with the block data of the first selected width, based upon an initial encryption or decryption key of a second selected width.

9. (Original) The apparatus of claim 3 further comprising: a round key generation circuit adapted to provide a round encryption or decryption key of the first selected width for combination with the block data of the first selected width, based upon an initial encryption or decryption key of a second selected width.

10. (Original) The apparatus of claim 4 further comprising: a round key generation circuit adapted to provide a round encryption or decryption key of the first selected width for combination with the block data of the first selected width, based upon an initial encryption or decryption key of a second selected width.

11. (Original) The apparatus of claim 5 further comprising: a round key generation circuit adapted to provide a round encryption or decryption key of the first selected width for combination with the block data of the first selected width, based upon an initial encryption or decryption key of a second selected width.

12. (Original) The apparatus of claim 6 further comprising: a round key generation circuit adapted to provide a round encryption or decryption key of the first selected width for combination with the block data of the first selected width, based upon an initial encryption or decryption key of a second selected width.

13. (Original) The apparatus of claim 7, further comprising: the round key generation circuit being adapted to generate each round key by the expansion of a starting key of a second selected width.

14. (Original) The apparatus of claim 8, further comprising: the round key generation circuit being adapted to generate each round key by the expansion of a starting key of a second selected width.

15. (Original) The apparatus of claim 9, further comprising: the round key generation circuit being adapted to generate each round key by the expansion of a starting key of a second selected width.

16. (Original) The apparatus of claim 10, further comprising: the round key generation circuit being adapted to generate each round key by the expansion of a starting key of a second selected width.

17. (Original) The apparatus of claim 11, further comprising: the round key generation circuit being adapted to generate each round key by the expansion of a starting key of a second selected width.

18. (Original) The apparatus of claim 12, further comprising: the round key generation circuit being adapted to generate each round key by the expansion of a starting key of a second selected width.

19. (Original) The apparatus of claim 13, further comprising: the second selected width equals the first selected width.

20. (Original) The apparatus of claim 14, further comprising: the second selected width equals the first selected width.

21. (Original) The apparatus of claim 15, further comprising: the second selected width equals the first selected width.

22. (Original) The apparatus of claim 16, further comprising: the second selected width equals the first selected width.

23. (Original) The apparatus of claim 17, further comprising: the second selected width equals the first selected width.

24. (Original) The apparatus of claim 18, further comprising: the second selected width equals the first selected width.

25. (Original) The apparatus of claim 19 further comprising: the encryption circuit is adapted to perform an affine transformation and the decryption circuit is adapted to perform an inverse of the affine transformation.

26. (Original) The apparatus of claim 20 further comprising: the encryption circuit is adapted to perform an affine transformation and the decryption circuit is adapted to perform an inverse of the amine transformation.

27. (Original) The apparatus of claim 21 further comprising: the encryption circuit is adapted to perform an affine transformation and the decryption circuit is adapted to perform an inverse of the affine transformation.

28. (Original) The apparatus of claim 22 further comprising: the encryption circuit is adapted to perform an affine transformation and the decryption circuit is adapted to perform an inverse of the amine transformation.

29. (Original) The apparatus of claim 23 further comprising: the encryption circuit is adapted to perform an affine transformation and the decryption circuit is adapted to perform an inverse of the affine transformation.

30. (Original) The apparatus of claim 24 further comprising: the encryption circuit is adapted to perform an affine transformation and the decryption circuit is adapted to perform an inverse of the affine transformation.

31. (Original) An encryption/decryption circuit comprising: a staged pipelined logic circuit adapted to perform in series stages of encryption/decryption operations on a stage data block of a first selected width utilizing an encryption/decryption key of the first selected width and to provide an output data block of the first selected width, comprising a subsequent stage input data block input to a subsequent stage of the staged pipelined logic circuit;

a stage input data block buffer adapted to hold the stage input data block for input into a stage of the staged pipelined logic circuit, the input data block having the first selected width;

an encryption circuit adapted to encrypt the stage input data block into a encrypted stage input data block having the first selected width, the encrypted stage input data block comprising a unique combination of data bits for each unique combination of data bits in the stage input data block of the first selected width, and the encrypted stage input data block forming an input to a stage substitution circuit, the output of the stage substitution circuit forming a first subsequent stage input data block for a subsequent stage of the staged pipelined logic circuit;

a decryption circuit adapted to decrypt the stage input data block into a decrypted stage input data block having the first selected width, the decrypted stage input data block comprising a unique combination of data bits for each unique combination of data bits in the stage input data block of the first selected width that is the inverse of the encryption performed by the encryption circuit, the decrypted stage input data block forming a second subsequent stage input to the substitution circuit;

a first selector circuit adapted to select as the input to the substitution circuit the first or the second input; and,

a second selector circuit adapted to select as the subsequent stage input data block for the subsequent stage of the staged pipelined logic circuit the output of the substitution circuit or the stage input data block.

32. (Original) An encryption/decryption circuit comprising: a staged pipelined logic circuit adapted to perform in series stages of encryption/decryption operations on a stage data block of a first selected width utilizing an encryption/decryption key of the first selected width and to provide an output data block of the first selected width, comprising a subsequent stage input data block input to a subsequent stage of the staged pipelined logic circuit;

a stage input data block buffer adapted to hold the stage input data block for input into a stage of the staged pipelined logic circuit, the input data block having the first selected width;

an encryption circuit adapted to encrypt the stage input data block into a encrypted stage input data block having the first selected width, the encrypted stage input data block comprising a unique combination of data bits for each unique combination of data bits in the stage input data block of the first selected width, and the encrypted stage input data block forming an input to a stage substitution circuit, the output of the stage substitution circuit forming a first subsequent stage input data block for a subsequent stage of the staged pipelined logic circuit;

a decryption circuit adapted to decrypt the stage input data block into a decrypted stage input data block having the first selected width, the decrypted stage input data block comprising a unique combination of data bits for each unique combination of data bits in the stage input data block of the first selected width that is the inverse of the encryption performed by the encryption circuit, the decrypted stage input data block forming a second subsequent stage input to the substitution circuit;

a first selector circuit adapted to select as the input to the substitution circuit the first or the second input;

a second selector circuit adapted to select as the subsequent stage input data block for the subsequent stage of the staged pipelined logic circuit the output of the substitution circuit or the stage input data block; and,

the staged pipelined logic circuit being further adapted to perform in series the stages of the encryption/decryption operations in a first plurality of stages of the staged pipelined logic circuit, each of the stages of the first plurality of stages comprising a round, and to repeat this operation for a selected number of times and for a selected number of rounds each of the selected number of times, to thereby effect a total number of rounds.

33. (Original) An encryption/decryption circuit comprising: a staged pipelined logic circuit adapted to perform in series stages of encryption/decryption operations on a stage data block of a first selected width utilizing an encryption/decryption key of the first selected width and to provide an output data block of the first selected width, comprising a subsequent stage input data block input to a subsequent stage of the staged pipelined logic circuit;

a stage input data block buffer adapted to hold the stage input data block for input into a stage of the staged pipelined logic circuit, the input data block having the first selected width;

an encryption circuit adapted to encrypt the stage input data block into a encrypted stage input data block having the first selected width, the encrypted stage input data block comprising a unique combination of data bits for each unique combination of data bits in the stage input data block of the first selected width, and the encrypted stage input data block forming an input to a stage substitution circuit, the output of the stage substitution circuit forming a first subsequent stage input data block for a subsequent stage of the staged pipelined logic circuit;

a decryption circuit adapted to decrypt the stage input data block into a decrypted stage input data block having the first selected width, the decrypted stage input data block comprising a unique combination of data bits for each unique combination of data bits in the stage input data block of the first selected width that is the inverse of the encryption performed by the encryption circuit, the decrypted stage input data block forming a second subsequent stage input to the substitution circuit;

a first selector circuit adapted to select as the input to the substitution circuit the first or the second input;

a second selector circuit adapted to select as the subsequent stage input data block for the subsequent stage of the staged pipelined logic circuit the output of the substitution circuit or the stage input data block;

the staged pipelined logic circuit being further adapted to perform in series the stages of the encryption/decryption operations in a first plurality of stages of the staged pipelined logic circuit, each of the stages of the first plurality of stages comprising a round, and to repeat this operation for a selected number of times and for a selected number of rounds each of the selected number of times, to thereby effect a total number of rounds; and,

the staged pipelined logic circuit being further adapted to perform in any given one of the first plurality of times less than the first plurality of rounds depending upon the total number of rounds necessary.

34. (Original) An encryption/decryption circuit comprising: a staged pipelined logic circuit adapted to perform in series stages of encryption/decryption operations on a stage data block of a first selected width utilizing an encryption/decryption key of the first selected width and to provide an output data block of the first selected width, comprising a subsequent stage input data block input to a subsequent stage of the staged pipelined logic circuit;

a stage input data block buffer adapted to hold the stage input data block for input into a stage of the staged pipelined logic circuit, the input data block having the first selected width;

an encryption circuit adapted to encrypt the stage input data block into a encrypted stage input data block having the first selected width, the encrypted stage input data block comprising a unique combination of data bits for each unique combination of data bits in the stage input data block of the first selected width, and the encrypted stage input data block forming an input to a stage substitution circuit, the output of the stage substitution circuit forming a first subsequent stage input data block for a subsequent stage of the staged pipelined logic circuit;

a decryption circuit adapted to decrypt the stage input data block into a decrypted stage input data block having the first selected width, the decrypted stage input data block comprising a unique combination of data bits for each unique combination of data bits in the stage input data block of the first selected width that is the inverse of the encryption performed by the encryption circuit, the decrypted stage input data block forming a second subsequent stage input to the substitution circuit;

a first selector circuit adapted to select as the input to the substitution circuit the first or the second input; .

a second selector circuit adapted to select as the subsequent stage input data block for the subsequent stage of the staged pipelined logic circuit the output of the substitution circuit or the stage input data block;

the staged pipelined logic circuit being further adapted to perform in series the stages of the encryption/decryption operations in a first plurality of stages of the staged pipelined logic circuit, each of the stages of the first plurality of stages comprising a round, and to repeat this operation for a selected number of times and for a selected number of rounds each of the selected number of times, to thereby effect a total number of rounds;

the staged pipelined logic circuit being further adapted to perform in any given one of the first plurality of times less than the first plurality of rounds depending upon the total number of rounds necessary; and,

a round key generation circuit adapted to provide a round encryption or decryption key of the first selected width for combination with the block data of the first selected width, based upon an initial encryption or decryption key of a second selected width.

35. (Original) An encryption/decryption circuit comprising: a staged pipelined logic circuit adapted to perform in series stages of encryption/decryption operations on a stage data block of a first selected width utilizing an encryption/decryption key of the first selected width and to provide an output data block of the first selected width, comprising a subsequent stage input data block input to a subsequent stage of the staged pipelined logic circuit;

a stage input data block buffer adapted to hold the stage input data block for input into a stage of the staged pipelined logic circuit, the input data block having the first selected width;

an encryption circuit adapted to encrypt the stage input data block into a encrypted stage input data block having the first selected width, the encrypted stage input data block comprising a unique combination of data bits for each unique combination of data bits in the stage input data block of the first selected width, and the encrypted stage input data block forming an input to a stage substitution circuit, the output of the stage substitution circuit forming a first subsequent stage input data block for a subsequent stage of the staged pipelined logic circuit;

a decryption circuit adapted to decrypt the stage input data block into a decrypted stage input data block having the first selected width, the decrypted stage input data block comprising a unique combination of data bits for each unique combination of data bits in the stage input data block of the first selected width that is the inverse of the encryption performed by the encryption circuit, the decrypted stage input data block forming a second subsequent stage input to the substitution circuit;

a first selector circuit adapted to select as the input to the substitution circuit the first or the second input;

a second selector circuit adapted to select as the subsequent stage input data block for the subsequent stage of the staged pipelined logic circuit the output of the substitution circuit or the stage input data block;

the staged pipelined logic circuit being further adapted to perform in series the stages of the encryption/decryption operations in a first plurality of stages of the staged pipelined logic circuit, each of the stages of the first plurality of stages comprising a round, and to repeat this operation for a selected number of times and for a selected number of rounds each of the selected number of times, to thereby effect a total number of rounds;

the staged pipelined logic circuit being further adapted to perform in any given one of the first plurality of times less than the first plurality of rounds depending upon the total number of rounds necessary;

a round key generation circuit adapted to provide a round encryption or decryption key of the first selected width for combination with the block data of the first selected width, based upon an initial encryption or decryption key of a second selected width; and,

the round key generation circuit being adapted to generate each round key by the expansion of a starting key of a second selected width.

36. (Original) An encryption/decryption circuit comprising: a staged pipelined logic circuit adapted to perform in series stages of encryption/decryption operations on a stage data block of a first selected width utilizing an encryption/decryption key of the first selected width and to provide an output data block of the first selected width, comprising a subsequent stage input data block input to a subsequent stage of the staged pipelined logic circuit;

a stage input data block buffer adapted to hold the stage input data block for input into a stage of the staged pipelined logic circuit, the input data block having the first selected width;

an encryption circuit adapted to encrypt the stage input data block into a encrypted stage input data block having the first selected width, the encrypted stage input data block comprising a unique combination of data bits for each unique combination of data bits in the stage input data block of the first selected width, and the encrypted stage input data block forming an input to a stage substitution circuit, the output of the stage substitution circuit forming a first subsequent stage input data block for a subsequent stage of the staged pipelined logic circuit;

a decryption circuit adapted to decrypt the stage input data block into a decrypted stage input data block having the first selected width, the decrypted stage input data block comprising a unique combination of data bits for each unique combination of data bits in the stage input data block of the first selected width that is the inverse of the encryption performed by the encryption circuit, the decrypted stage input data block forming a second subsequent stage input to the substitution circuit;

a first selector circuit adapted to select as the input to the substitution circuit the first or the second input;

a second selector circuit adapted to select as the subsequent stage input data block for the subsequent stage of the staged pipelined logic circuit the output of the substitution circuit or the stage input data block;

the staged pipelined logic circuit being further adapted to perform in series the stages of the encryption/decryption operations in a first plurality of stages of the staged pipelined logic circuit, each of the stages of the first plurality of stages comprising a round, and to repeat this operation for a selected number of times and for a selected number of rounds each of the selected number of times, to thereby effect a total number of rounds;

the staged pipelined logic circuit being further adapted to perform in any given one of the first plurality of times less than the first plurality of rounds depending upon the total number of rounds necessary;

a round key generation circuit adapted to provide a round encryption or decryption key of the first selected width for combination with the block data of the first selected width, based upon an initial encryption or decryption key of a second selected width; and,

the round key generation circuit being adapted to generate each round key by the expansion of a starting key of a second selected width, equal to the first selected width.

37. (Original) An encryption/decryption circuit comprising: a staged pipelined logic circuit adapted to perform in series stages of encryption/decryption operations on a stage data block of a first selected width utilizing an encryption/decryption key of the first selected width and to provide an output data block of the first selected width, comprising a subsequent stage input data block input to a subsequent stage of the staged pipelined logic circuit;

a stage input data block buffer adapted to hold the stage input data block for input into a stage of the staged pipelined logic circuit, the input data block having the first selected width;

an encryption circuit adapted to encrypt the stage input data block into a encrypted stage input data block having the first selected width, the encrypted stage input data block comprising a unique combination of data bits for each unique combination of data bits in the stage input data block of the first selected width, and the encrypted stage input data block forming an input to a stage substitution circuit, the output of the stage substitution circuit forming a first subsequent stage input data block for a subsequent stage of the staged pipelined logic circuit;

a decryption circuit adapted to decrypt the stage input data block into a decrypted stage input data block having the first selected width, the decrypted stage input data block comprising a unique combination of data bits for each unique combination of data bits in the stage input data block of the first selected width that is the inverse of the encryption performed by the encryption circuit, the decrypted stage input data block forming a second subsequent stage input to the substitution circuit;

a first selector circuit adapted to select as the input to the substitution circuit the first or the second input;

a second selector circuit adapted to select as the subsequent stage input data block for the subsequent stage of the staged pipelined logic circuit the output of the substitution circuit or the stage input data block;

the staged pipelined logic circuit being further adapted to perform in series the stages of the encryption/decryption operations in a first plurality of stages of the staged pipelined logic circuit, each of the stages of the first plurality of stages comprising a round, and to repeat this operation for a selected number of times and for a selected number of rounds each of the selected number of times, to thereby effect a total number of rounds;

the staged pipelined logic circuit being further adapted to perform in any given one of the first plurality of times less than the first plurality of rounds depending upon the total number of rounds necessary;

a round key generation circuit adapted to provide a round encryption or decryption key of the first selected width for combination with the block data of the first selected width, based upon an initial encryption or decryption key of a second selected width;

the round key generation circuit being adapted to generate each round key by the expansion of a starting key of a second selected width, equal to the first selected width; and,

the encryption circuit is adapted to perform an affine transformation and the decryption circuit is adapted to perform an inverse of the affine transformation.

38. (Original) An encryption/decryption circuit comprising: a staged pipelined logic circuit means for performing in series stages of encryption/decryption operations on a stage data block of a first selected width utilizing an encryption/decryption key of the first selected width and providing an output data block of the first selected width, comprising a subsequent stage input data block input to a subsequent stage of the staged pipelined logic circuit;

a stage input data block buffer means for holding the stage input data block for input into a stage of the staged pipelined logic circuit, the input data block having the first selected width;

an encryption circuit means for encrypting the stage input data block into a encrypted stage input data block having the first selected width, the encrypted stage input data block comprising a unique combination of data bits for each unique combination of data bits in the stage input data block of the first selected width, and the encrypted stage input data block forming an input to a stage substitution circuit, the output of the stage substitution circuit forming a first subsequent stage input data block for a subsequent stage of the staged pipelined logic circuit means;

a decryption circuit means for decrypting the stage input data block into a decrypted stage input data block having the first selected width, the decrypted stage input data block comprising a unique combination of data bits for each unique combination of data bits in the stage input data block of the first selected width that is the inverse of the encryption performed by the encryption circuit, the decrypted stage input data block forming a second subsequent stage input to the substitution circuit; and,

a first selector circuit means for selecting as the input to the substitution circuit the first or the second input.

39. (Original) The apparatus of claim 38, further comprising: a second selector circuit means for selecting as the subsequent stage input data block for the subsequent stage of the staged pipelined logic circuit means the output of the substitution circuit or the stage input data block.

40. (Original) The apparatus of claim 38 further comprising: the staged pipelined logic circuit means further including means for performing in series the stages of the

encryption/decryption operations in a first plurality of stages of the staged pipelined logic circuit means, each of the stages of the first plurality of stages comprising a round, and for repeating this operation for a selected number of times and for a selected number of rounds each of the selected number of times, to thereby effect a total number of rounds.

41. (Original) The apparatus of claim 39 further comprising: the staged pipelined logic circuit means further including means for performing in series the stages of the encryption/decryption operations in a first plurality of stages of the staged pipelined logic circuit means, each of the stages of the first plurality of stages comprising a round, and for repeating this operation for a selected number of times and for a selected number of rounds each of the selected number of times, to thereby effect a total number of rounds.

42. (Original) The apparatus of claim 40 further comprising: the staged pipelined logic circuit means further comprising means for performing in any given one of the first plurality of times less than the first plurality of rounds depending upon the total number of rounds necessary.

43. (Original) The apparatus of claim 41 further comprising: the staged pipelined logic circuit means further comprising means for performing in any given one of the first plurality of times less than the first plurality of rounds depending upon the total number of rounds necessary.

44. (Original) The apparatus of claim 38 further comprising: a round key generation circuit means for providing a round encryption or decryption key of the first selected width for combination with the block data of the first selected width, based upon an initial encryption or decryption key of a second selected width.

45. (Original) The apparatus of claim 39 further comprising: a round key generation circuit means for providing a round encryption or decryption key of the first selected width for combination

with the block data of the first selected width, based upon an initial encryption or decryption key of a second selected width.

46. (Original) The apparatus of claim 40 further comprising: a round key generation circuit means for providing a round encryption or decryption key of the first selected width for combination with the block data of the first selected width, based upon an initial encryption or decryption key of a second selected width.

47. (Original) The apparatus of claim 41 further comprising: a round key generation circuit means for providing a round encryption or decryption key of the first selected width for combination with the block data of the first selected width, based upon an initial encryption or decryption key of a second selected width.

48. (Original) The apparatus of claim 42 further comprising: a round key generation circuit means for providing a round encryption or decryption key of the first selected width for combination with the block data of the first selected width, based upon an initial encryption or decryption key of a second selected width.

49. (Original) The apparatus of claim 43 further comprising: a round key generation circuit means for providing a round encryption or decryption key of the first selected width for combination with the block data of the first selected width, based upon an initial encryption or decryption key of a second selected width.

50. (Original) The apparatus of claim 44, further comprising: the round key generation circuit means further including means for generating each round key by the expansion of a starting key of a second selected width.

51. (Original) The apparatus of claim 45, further comprising: the round key generation circuit means further including means for generating each round key by the expansion of a starting key of a second selected width.

52. (Original) The apparatus of claim 46, further comprising: the round key generation circuit means further including means for generating each round key by the expansion of a starting key of a second selected width.

53. (Original) The apparatus of claim 47, further comprising: the round key generation circuit means further including means for generating each round key by the expansion of a starting key of a second selected width.

54. (Original) The apparatus of claim 48, further comprising: the round key generation circuit means further including means for generating each round key by the expansion of a starting key of a second selected width.

55. (Original) The apparatus of claim 49, further comprising: the round key generation circuit means further including means for generating each round key by the expansion of a starting key of a second selected width.

56. (Original) The apparatus of claim 50, further comprising: the second selected width equals the first selected width.

57. (Original) The apparatus of claim 51, further comprising: the second selected width equals the first selected width.

58. (Original) The apparatus of claim 52, further comprising: the second selected width equals the first selected width.

59. (Original) The apparatus of claim 53, further comprising: the second selected width equals the first selected width.

60. (Original) The apparatus of claim 54, further comprising: the second selected width equals the first selected width.

61. (Original) The apparatus of claim 55, further comprising: the second selected width equals the first selected width.

62. (Original) The apparatus of claim 56 further comprising: the encryption circuit means further includes means for performing an affine transformation and the decryption circuit means further includes means for performing an inverse of the affine transformation.

63. (Original) The apparatus of claim 57 further comprising: the encryption circuit means further includes means for performing an affine transformation and the decryption circuit means further includes means for performing an inverse of the affine transformation.

64. (Original) The apparatus of claim 58 further comprising: the encryption circuit means further includes means for performing an affine transformation and the decryption circuit means further includes means for performing an inverse of the affine transformation.

65. (Original) The apparatus of claim 59 further comprising: the encryption circuit means further includes means for performing an affine transformation and the decryption circuit means further includes means for performing an inverse of the affine transformation.

66. (Original) The apparatus of claim 60 further comprising: the encryption circuit means further includes means for performing an affine transformation and the decryption circuit means further includes means for performing an inverse of the affine transformation.

67. (Original) The apparatus of claim 61 further comprising: the encryption circuit means further includes means for performing an affine transformation and the decryption circuit means further includes means for performing an inverse of the affine transformation.

68. (Original) An encryption/decryption circuit comprising: a staged pipelined logic circuit means for performing in series stages of encryption/decryption operations on a stage data block of a first selected width utilizing an encryption/decryption key of the first selected width and providing an output data block of the first selected width, comprising a subsequent stage input data block input to a subsequent stage of the staged pipelined logic circuit;

a stage input data block buffer means for holding the stage input data block for input into a stage of the staged pipelined logic circuit, the input data block having the first selected width;

an encryption circuit means for encrypting the stage input data block into a encrypted stage input data block having the first selected width, the encrypted stage input data block comprising a unique combination of data bits for each unique combination of data bits in the stage input data block of the first selected width, and the encrypted stage input data block forming an input to a stage substitution circuit, the output of the stage substitution circuit forming a first subsequent stage input data block for a subsequent stage of the staged pipelined logic circuit means;

a decryption circuit means for decrypting the stage input data block into a decrypted stage input data block having the first selected width, the decrypted stage input data block comprising a unique combination of data bits for each unique combination of data bits in the stage input data block of the first selected width that is the inverse of the encryption performed by the encryption circuit, the decrypted stage input data block forming a second subsequent stage input to the substitution circuit;

a first selector circuit means for selecting as the input to the substitution circuit the first or the second input; and,

a second selector circuit means for selecting as the subsequent stage input data block for the subsequent stage of the staged pipelined logic circuit means the output of the substitution circuit or the stage input data block.

69. (Original) An encryption/decryption circuit comprising: a staged pipelined logic circuit means for performing in series stages of encryption/decryption operations on a stage data block of a first selected width utilizing an encryption/decryption key of the first selected width and providing an output data block of the first selected width, comprising a subsequent stage input data block input to a subsequent stage of the staged pipelined logic circuit;

a stage input data block buffer means for holding the stage input data block for input into a stage of the staged pipelined logic circuit, the input data block having the first selected width;

an encryption circuit means for encrypting the stage input data block into a encrypted stage input data block having the first selected width, the encrypted stage input data block comprising a unique combination of data bits for each unique combination of data bits in the stage input data block of the first selected width, and the encrypted stage input data block forming an input to a stage substitution circuit, the output of the stage substitution circuit forming a first subsequent stage input data block for a subsequent stage of the staged pipelined logic circuit means;

a decryption circuit means for decrypting the stage input data block into a decrypted stage input data block having the first selected width, the decrypted stage input data block comprising a unique combination of data bits for each unique combination of data bits in the stage input data block of the first selected width that is the inverse of the encryption performed by the encryption circuit, the decrypted stage input data block forming a second subsequent stage input to the substitution circuit;

a first selector circuit means for selecting as the input to the substitution circuit the first or the second input;

a second selector circuit means for selecting as the subsequent stage input data block for the subsequent stage of the staged pipelined logic circuit means the output of the substitution circuit or the stage input data block; and,

the staged pipelined logic circuit means further including means for performing in series the stages of the encryption/decryption operations in a first plurality of stages of the staged pipelined logic circuit means, each of the stages of the first plurality of stages comprising a round, and for repeating this operation for a selected number of times and for a selected number of rounds each of the selected number of times, to thereby effect a total number of rounds.

70. (Original) An encryption/decryption circuit comprising: a staged pipelined logic circuit means for performing in series stages of encryption/decryption operations on a stage data block of a first selected width utilizing an encryption/decryption key of the first selected width and providing an output data block of the first selected width, comprising a subsequent stage input data block input to a subsequent stage of the staged pipelined logic circuit;

a stage input data block buffer means for holding the stage input data block for input into a stage of the staged pipelined logic circuit, the input data block having the first selected width;

an encryption circuit means for encrypting the stage input data block into a encrypted stage input data block having the first selected width, the encrypted stage input data block comprising a unique combination of data bits for each unique combination of data bits in the stage input data block of the first selected width, and the encrypted stage input data block forming an input to a stage substitution circuit, the output of the stage substitution circuit forming a first subsequent stage input data block for a subsequent stage of the staged pipelined logic circuit means;

a decryption circuit means for decrypting the stage input data block into a decrypted stage input data block having the first selected width, the decrypted stage input data block comprising a unique combination of data bits for each unique combination of data bits in the stage input data block of the first selected width that is the inverse of the encryption performed by the encryption circuit, the decrypted stage input data block forming a second subsequent stage input to the substitution circuit;

a first selector circuit means for selecting as the input to the substitution circuit the first or the second input;

a second selector circuit means for selecting as the subsequent stage input data block for the subsequent stage of the staged pipelined logic circuit means the output of the substitution circuit or the stage input data block;

the staged pipelined logic circuit means further including means for performing in series the stages of the encryption/decryption operations in a first plurality of stages of the staged pipelined logic circuit means, each of the stages of the first plurality of stages comprising a round, and for repeating this operation for a selected number of times and for a selected number of rounds each of the selected number of times, to thereby effect a total number of rounds; and,

the staged pipelined logic circuit means further comprising means for performing in any given one of the first plurality of times less than the first plurality of rounds depending upon the total number of rounds necessary.

71. (Original) An encryption/decryption circuit comprising: a staged pipelined logic circuit means for performing in series stages of encryption/decryption operations on a stage data block of a first selected width utilizing an encryption/decryption key of the first selected width and providing an output data block of the first selected width, comprising a subsequent stage input data block input to a subsequent stage of the staged pipelined logic circuit, a stage input data block buffer means for holding the stage input data block for input into a stage of the staged pipelined logic circuit, the input data block having the first selected width;

an encryption circuit means for encrypting the stage input data block into a encrypted stage input data block having the first selected width, the encrypted stage input data block comprising a unique combination of data bits for each unique combination of data bits in the stage input data block of the first selected width, and the encrypted stage input data block forming an input to a stage substitution circuit, the output of the stage substitution circuit forming a first subsequent stage input data block for a subsequent stage of the staged pipelined logic circuit means;

a decryption circuit means for decrypting the stage input data block into a decrypted stage input data block having the first selected width, the decrypted stage input data block comprising a unique combination of data bits for each unique combination of data bits in the stage input data block of the first selected width that is the inverse of the encryption performed by the encryption circuit, the decrypted stage input data block forming a second subsequent stage input to the substitution circuit;

a first selector circuit means for selecting as the input to the substitution circuit the first or the second input;

a second selector circuit means for selecting as the subsequent stage input data block for the subsequent stage of the staged pipelined logic circuit means the output of the substitution circuit or the stage input data block;

the staged pipelined logic circuit means further including means for performing in series the stages of the encryption/decryption operations in a first plurality of stages of the staged pipelined logic circuit means, each of the stages of the first plurality of stages comprising a round, and for repeating this operation for a selected number of times and for a selected number of rounds each of the selected number of times, to thereby effect a total number of rounds;

the staged pipelined logic circuit means further comprising means for performing in any given one of the first plurality of times less than the first plurality of rounds depending upon the total number of rounds necessary; and,

a round key generation circuit means for providing a round encryption or decryption key of the first selected width for combination with the block data of the first selected width, based upon an initial encryption or decryption key of a second selected width.

72. (Original) An encryption/decryption circuit comprising: a staged pipelined logic circuit means for performing in series stages of encryption/decryption operations on a stage data block of a first selected width utilizing an encryption/decryption key of the first selected width and providing an output data block of the first selected width, comprising a subsequent stage input data block input to a subsequent stage of the staged pipelined logic circuit, a stage input data block buffer means for

holding the stage input data block for input into a stage of the staged pipelined logic circuit, the input data block having the first selected width;

an encryption circuit means for encrypting the stage input data block into a encrypted stage input data block having the first selected width, the encrypted stage input data block comprising a unique combination of data bits for each unique combination of data bits in the stage input data block of the first selected width, and the encrypted stage input data block forming an input to a stage substitution circuit, the output of the stage substitution circuit forming a first subsequent stage input data block for a subsequent stage of the staged pipelined logic circuit means;

a decryption circuit means for decrypting the stage input data block into a decrypted stage input data block having the first selected width, the decrypted stage input data block comprising a unique combination of data bits for each unique combination of data bits in the stage input data block of the first selected width that is the inverse of the encryption performed by the encryption circuit, the decrypted stage input data block forming a second subsequent stage input to the substitution circuit;

a first selector circuit means for selecting as the input to the substitution circuit the first or the second input;

a second selector circuit means for selecting as the subsequent stage input data block for the subsequent stage of the staged pipelined logic circuit means the output of the substitution circuit or the stage input data block;

the staged pipelined logic circuit means further including means for performing in series the stages of the encryption/decryption operations in a first plurality of stages of the staged pipelined logic circuit means, each of the stages of the first plurality of stages comprising a round, and for repeating this operation for a selected number of times and for a selected number of rounds each of the selected number of times, to thereby effect a total number of rounds;

the staged pipelined logic circuit means further comprising means for performing in any given one of the first plurality of times less than the first plurality of rounds depending upon the total number of rounds necessary;

a round key generation circuit means for providing a round encryption or decryption key of the first selected width for combination with the block data of the first selected width, based upon an initial encryption or decryption key of a second selected width; and,

the round key generation circuit means further including means for generating each round key by the expansion of a starting key of a second selected width.

73. (Original) An encryption/decryption circuit comprising: a staged pipelined logic circuit means for performing in series stages of encryption/decryption operations on a stage data block of a first selected width utilizing an encryption/decryption key of the first selected width and providing an output data block of the first selected width, comprising a subsequent stage input data block input to a subsequent stage of the staged pipelined logic circuit;

a stage input data block buffer means for holding the stage input data block for input into a stage of the staged pipelined logic circuit, the input data block having the first selected width;

an encryption circuit means for encrypting the stage input data block into a encrypted stage input data block having the first selected width, the encrypted stage input data block comprising a unique combination of data bits for each unique combination of data bits in the stage input data block of the first selected width, and the encrypted stage input data block forming an input to a stage substitution circuit, the output of the stage substitution circuit forming a first subsequent stage input data block for a subsequent stage of the staged pipelined logic circuit means;

a decryption circuit means for decrypting the stage input data block into a decrypted stage input data block having the first selected width, the decrypted stage input data block comprising a unique combination of data bits for each unique combination of data bits in the stage input data block of the first selected width that is the inverse of the encryption performed by the encryption circuit, the decrypted stage input data block forming a second subsequent stage input to the substitution circuit;

a first selector circuit means for selecting as the input to the substitution circuit the first or the second input;

a second selector circuit means for selecting as the subsequent stage input data block for the subsequent stage of the staged pipelined logic circuit means the output of the substitution circuit or the stage input data block;

the staged pipelined logic circuit means further including means for performing in series the stages of the encryption/decryption operations in a first plurality of stages of the staged pipelined logic circuit means, each of the stages of the first plurality of stages comprising a round, and for repeating this operation for a selected number of times and for a selected number of rounds each of the selected number of times, to thereby effect a total number of rounds;

the staged pipelined logic circuit means further comprising means for performing in any given one of the first plurality of times less than the first plurality of rounds depending upon the total number of rounds necessary;

a round key generation circuit means for providing a round encryption or decryption key of the first selected width for combination with the block data of the first selected width, based upon an initial encryption or decryption key of a second selected width; and,

the round key generation circuit means further including means for generating each round key by the expansion of a starting key of a second selected width equal to the first selected width.

74. (Original) An encryption/decryption circuit comprising: a staged pipelined logic circuit means for performing in series stages of encryption/decryption operations on a stage data block of a first selected width utilizing an encryption/decryption key of the first selected width and providing an output data block of the first selected width, comprising a subsequent stage input data block input to a subsequent stage of the staged pipelined logic circuit;

a stage input data block buffer means for holding the stage input data block for input into a stage of the staged pipelined logic circuit, the input data block having the first selected width;

an encryption circuit means for encrypting the stage input data block into a encrypted stage input data block having the first selected width, the encrypted stage input data block comprising a unique combination of data bits for each unique combination of data bits in the stage input data block of the first selected width, and the encrypted stage input data block forming an input to a stage substitution circuit, the output of the stage substitution circuit forming a first subsequent stage input data block for a subsequent stage of the staged pipelined logic circuit means;

a decryption circuit means for decrypting the stage input data block into a decrypted stage input data block having the first selected width, the decrypted stage input data block comprising a unique combination of data bits for each unique combination of data bits in the stage input data block of the first selected width that is the inverse of the encryption performed by the encryption circuit, the decrypted stage input data block forming a second subsequent stage input to the substitution circuit;

a first selector circuit means for selecting as the input to the substitution circuit the first or the second input;

a second selector circuit means for selecting as the subsequent stage input data block for the subsequent stage of the staged pipelined logic circuit means the output of the substitution circuit or the stage input data block;

the staged pipelined logic circuit means further including means for performing in series the stages of the encryption/decryption operations in a first plurality of stages of the staged pipelined logic circuit means, each of the stages of the first plurality of stages comprising a round, and for repeating this operation for a selected number of times and for a selected number of rounds each of the selected number of times, to thereby effect a total number of rounds;

the staged pipelined logic circuit means further comprising means for performing in any given one of the first plurality of times less than the first plurality of rounds depending upon the total number of rounds necessary;

a round key generation circuit means for providing a round encryption or decryption key of the first selected width for combination with the block data of the first selected width, based upon an initial encryption or decryption key of a second selected width;

the round key generation circuit means further including means for generating each round key by the expansion of a starting key of a second selected width equal to the first selected width; and, the encryption circuit means further includes means for performing an affine transformation and the decryption circuit means further includes means for performing an inverse of the affine transformation.

75. (Original) An encryption/decryption method comprising: performing in series stages of encryption/decryption operations on a stage data block of a first selected width utilizing an encryption/decryption key of the first selected width and providing an output data block of the first selected width, comprising a subsequent stage input data block input to a subsequent stage of the series of stages;

holding the stage input data block for input into a stage of the series of stages, the input data block having the first selected width;

encrypting the stage input data block into a encrypted stage input data block having the first selected width, the encrypted stage input data block comprising a unique combination of data bits for each unique combination of data bits in the stage input data block of the first selected width;

decrypting the stage input data block into a decrypted stage input data block having the first selected width, the decrypted stage input data block comprising a unique combination of data bits for each unique combination of data bits in the stage input data block of the first selected width that is the inverse of the encryption performed by the encryption step; and,

performing a substitution operation on either the encrypted stage input data block or the decrypted stage input data block.

76. (Original) The method of claim 75, further comprising: selecting as a subsequent stage input data block for the subsequent stage of the series of stages the output of the substitution step or the stage input data block.

77. (Original) The method of claim 76 further comprising: performing in series the stages of the encryption/decryption operations in a first plurality of stages of the series of stages, each of the stages of the first plurality of stages comprising a round, and repeating this operation for a selected

number of times and for a selected number of rounds each of the selected number of times, to thereby effect a total number of rounds.

78. (Original) The method of claim 76 further comprising: performing in series the stages of the encryption/decryption operations in a first plurality of stages of the series of stages, each of the stages of the first plurality of stages comprising a round, and repeating this operation for a selected number of times and for a selected number of rounds each of the selected number of times, to thereby effect a total number of rounds.

79. (Original) The method of claim 77 further comprising: performing in any given one of the first plurality of times less than the first plurality of rounds depending upon the total number of rounds necessary.

80. (Original) The method of claim 78 further comprising: performing in any given one of the first plurality of times less than the first plurality of rounds depending upon the total number of rounds necessary.

81. (Original) The apparatus of claim 75 further comprising: providing a round encryption or decryption key of the first selected width for combination with the block data of the first selected width, based upon an initial encryption or decryption key of a second selected width.

82. (Original) The method of claim 76 further comprising: providing a round encryption or decryption key of the first selected width for combination with the block data of the first selected width, based upon an initial encryption or decryption key of a second selected width.

83. (Original) The method of claim 77 further comprising: providing a round encryption or decryption key of the first selected width for combination with the block data of the first selected width, based upon an initial encryption or decryption key of a second selected width.

84. (Original) The method of claim 78 further comprising: providing a round encryption or decryption key of the first selected width for combination with the block data of the first selected width, based upon an initial encryption or decryption key of a second selected width.

85. (Original) The method of claim 79 further comprising: providing a round encryption or decryption key of the first selected width for combination with the block data of the first selected width, based upon an initial encryption or decryption key of a second selected width.

86. (Original) The method of claim 80 further comprising: providing a round encryption or decryption key of the first selected width for combination with the block data of the first selected width, based upon an initial encryption or decryption key of a second selected width.

87. (Original) The method of claim 81, further comprising: generating each round key by the expansion of a starting key of a second selected width.

88. (Original) The method of claim 82, further comprising: generating each round key by the expansion of a starting key of a second selected width.

89. (Original) The method of claim 83, further comprising: generating each round key by the expansion of a starting key of a second selected width.

90. (Original) The method of claim 84, further comprising: generating each round key by the expansion of a starting key of a second selected width.

91. (Original) The method of claim 85, further comprising: generating each round key by the expansion of a starting key of a second selected width.

92. (Original) The method of claim 86, further comprising: generating each round key by the expansion of a starting key of a second selected width.

93. (Original) The method of claim 87, further comprising: the second selected width equals the first selected width.

94. (Original) The method of claim 88, further comprising: the second selected width equals the first selected width.

95. (Original) The method of claim 89, further comprising: the second selected width equals the first selected width.

96. (Original) The method of claim 90, further comprising: the second selected width equals the first selected width.

97. (Original) The method of claim 91, further comprising: the second selected width equals the first selected width.

98. (Original) The method of claim 92, further comprising: the second selected width equals the first selected width.

99. (Original) The method of claim 93 further comprising: the encryption step further includes performing an affine transformation and the decryption step further includes performing an inverse of the affine transformation.

100. (Original) The method of claim 94 further comprising: the encryption step further includes performing an affine transformation and the decryption step further includes performing an inverse of the affine transformation.

101. (Original) The method of claim 95 further comprising: the encryption step further includes performing an affine transformation and the decryption step further includes performing an inverse of the affine transformation.

102. (Original) The method of claim 96 further comprising: the encryption step further includes performing an affine transformation and the decryption step further includes performing an inverse of the affine transformation.

103. (Original) The method of claim 97 further comprising: the encryption step further includes performing an affine transformation and the decryption step further includes performing an inverse of the affine transformation.

104. (Original) The method of claim 98 further comprising: the encryption step further includes performing an affine transformation and the decryption step further includes performing an inverse of the affine transformation.

105. (Original) An encryption/decryption method comprising: performing in series stages of encryption/decryption operations on a stage data block of a first selected width utilizing an encryption/decryption key of the first selected width and providing an output data block of the first selected width, comprising a subsequent stage input data block input to a subsequent stage of the series of stages;

holding the stage input data block for input into a stage of the series of stages, the input data block having the first selected width;

encrypting the stage input data block into a encrypted stage input data block having the first selected width, the encrypted stage input data block comprising a unique combination of data bits for each unique combination of data bits in the stage input data block of the first selected width;

decrypting the stage input data block into a decrypted stage input data block having the first selected width, the decrypted stage input data block comprising a unique combination of data bits for each unique combination of data bits in the stage input data block of the first selected width that is the inverse of the encryption performed by the encryption step;

performing a substitution operation on either the encrypted stage input data block or the decrypted stage input data block; and,

selecting as a subsequent stage input data block for the subsequent stage of the series of stages the output of the substitution step or the stage input data block.

106. (Original) An encryption/decryption method comprising: performing in series stages of encryption/decryption operations on a stage data block of a first selected width utilizing an encryption/decryption key of the first selected width and providing an output data block of the first selected width, comprising a subsequent stage input data block input to a subsequent stage of the series of stages;

holding the stage input data block for input into a stage of the series of stages, the input data block having the first selected width;

encrypting the stage input data block into a encrypted stage input data block having the first selected width, the encrypted stage input data block comprising a unique combination of data bits for each unique combination of data bits in the stage input data block of the first selected width;

decrypting the stage input data block into a decrypted stage input data block having the first selected width, the decrypted stage input data block comprising a unique combination of data bits for each unique combination of data bits in the stage input data block of the first selected width that is the inverse of the encryption performed by the encryption step;

performing a substitution operation on either the encrypted stage input data block or the decrypted stage input data block;

selecting as a subsequent stage input data block for the subsequent stage of the series of stages the output of the substitution step or the stage input data block; and, performing in series the stages of the encryption/decryption operations in a first plurality of stages of the series of stages, each of the stages of the first plurality of stages comprising a round, and repeating this operation for a selected number of times and for a selected number of rounds each of the selected number of times, to thereby effect a total number of rounds.

107. (Original) An encryption/decryption method comprising: performing in series stages of encryption/decryption operations on a stage data block of a first selected width utilizing an encryption/decryption key of the first selected width and providing an output data block of the first selected width, comprising a subsequent stage input data block input to a subsequent stage of the series of stages;

holding the stage input data block for input into a stage of the series of stages, the input data block having the first selected width;

encrypting the stage input data block into a encrypted stage input data block having the first selected width, the encrypted stage input data block comprising a unique combination of data bits for each unique combination of data bits in the stage input data block of the first selected width;

decrypting the stage input data block into a decrypted stage input data block having the first selected width, the decrypted stage input data block comprising a unique combination of data bits for each unique combination of data bits in the stage input data block of the first selected width that is the inverse of the encryption performed by the encryption step;

performing a substitution operation on either the encrypted stage input data block or the decrypted stage input data block;

selecting as a subsequent stage input data block for the subsequent stage of the series of stages the output of the substitution step or the stage input data block;

performing in series the stages of the encryption/decryption operations in a first plurality of stages of the series of stages, each of the stages of the first plurality of stages comprising a round, and repeating this operation for a selected number of times and for a selected number of rounds each of the selected number of times, to thereby effect a total number of rounds; and, performing in any given one of the first plurality of times less than the first plurality of rounds depending upon the total number of rounds necessary.

108. (Original) An encryption/decryption method comprising: performing in series stages of encryption/decryption operations on a stage data block of a first selected width utilizing an encryption/decryption key of the first selected width and providing an output data block of the first selected width, comprising a subsequent stage input data block input to a subsequent stage of the series of stages;

holding the stage input data block for input into a stage of the series of stages, the input data block having the first selected width;

encrypting the stage input data block into a encrypted stage input data block having the first selected width, the encrypted stage input data block comprising a unique combination of data bits for each unique combination of data bits in the stage input data block of the first selected width;

decrypting the stage input data block into a decrypted stage input data block having the first selected width, the decrypted stage input data block comprising a unique combination of data bits for each unique combination of data bits in the stage input data block of the first selected width that is the inverse of the encryption performed by the encryption step;

performing a substitution operation on either the encrypted stage input data block or the decrypted stage input data block;

selecting as a subsequent stage input data block for the subsequent stage of the series of stages the output of the substitution step or the stage input data block;

performing in series the stages of the encryption/decryption operations in a first plurality of stages of the series of stages, each of the stages of the first plurality of stages comprising a round, and repeating this operation for a selected number of times and for a selected number of rounds each of the selected number of times, to thereby effect a total number of rounds;

performing in any given one of the first plurality of times less than the first plurality of rounds depending upon the total number of rounds necessary; and,

generating each round key by the expansion of a starting key of a second selected width.

109. (Original) An encryption/decryption method comprising: performing in series stages of encryption/decryption operations on a stage data block of a first selected width utilizing an encryption/decryption key of the first selected width and providing an output data block of the first selected width, comprising a subsequent stage input data block input to a subsequent stage of the series of stages;

holding the stage input data block for input into a stage of the series of stages, the input data block having the first selected width;

encrypting the stage input data block into a encrypted stage input data block having the first selected width, the encrypted stage input data block comprising a unique combination of data bits for each unique combination of data bits in the stage input data block of the first selected width;

decrypting the stage input data block into a decrypted stage input data block having the first selected width, the decrypted stage input data block comprising a unique combination of data bits for each unique combination of data bits in the stage input data block of the first selected width that is the inverse of the encryption performed by the encryption step;

performing a substitution operation on either the encrypted stage input data block or the decrypted stage input data block;

selecting as a subsequent stage input data block for the subsequent stage of the series of stages the output of the substitution step or the stage input data block;

performing in series the stages of the encryption/decryption operations in a first plurality of stages of the series of stages, each of the stages of the first plurality of stages comprising a round, and repeating this operation for a selected number of times and for a selected number of rounds each of the selected number of times, to thereby effect a total number of rounds;

performing in any given one of the first plurality of times less than the first plurality of rounds depending upon the total number of rounds necessary;

generating each round key by the expansion of a starting key of a second selected width; and, the second selected width equals the first selected width.

110. (Original) An encryption/decryption method comprising: performing in series stages of encryption/decryption operations on a stage data block of a first selected width utilizing an encryption/decryption key of the first selected width and providing an output data block of the first selected width, comprising a subsequent stage input data block input to a subsequent stage of the series of stages;

holding the stage input data block for input into a stage of the series of stages, the input data block having the first selected width;

encrypting the stage input data block into a encrypted stage input data block having the first selected width, the encrypted stage input data block comprising a unique combination of data bits for each unique combination of data bits in the stage input data block of the first selected width;

decrypting the stage input data block into a decrypted stage input data block having the first selected width, the decrypted stage input data block comprising a unique combination of data bits for each unique combination of data bits in the stage input data block of the first selected width that is the inverse of the encryption performed by the encryption step;

performing a substitution operation on either the encrypted stage input data block or the decrypted stage input data block;

selecting as a subsequent stage input data block for the subsequent stage of the series of stages the output of the substitution step or the stage input data block;

performing in series the stages of the encryption/decryption operations in a first plurality of stages of the series of stages, each of the stages of the first plurality of stages comprising a round, and repeating this operation for a selected number of times and for a selected number of rounds each of the selected number of times, to thereby effect a total number of rounds;

performing in any given one of the first plurality of times less than the first plurality of rounds depending upon the total number of rounds necessary;

generating each round key by the expansion of a starting key of a second selected width;

the second selected width equals the first selected width; and,

the encryption step further includes performing an affine transformation and the decryption step further includes performing an inverse of the affine transformation.